Modernization Cross-Project Security Requirements

Task Overview

The cross-project work in the past sixty days has assisted the modernization of SFA by performing an assessment of all the Modernization projects and the work needed to certify and accredit these new and changing systems. Most of this work has been performed during the development phase of the Systems Development Life Cycle and has added value by identifying future security thinking, including controls below the application layer. In addition, we have evaluated security in existing systems undergoing major modifications, such as the new Financial Management System. Our work with the Senior Technical Lead for Modernization led to a drawing of a potential Network Security Architecture following a DOD model of Defense in Depth. This multi-point discipline is not yet on the drawing board for modernization, but this team highly recommends an approach of this type be developed.

As a follow-up to the project security status survey we sent out in July, we held interviews during the month of August with each of the projects' managers to determine: where the system was in its development cycle and project plan, what the scope of each project was, what security work had already been implemented, and what security work remained to be done. The information collected from the 12 interviews and subsequent follow-on discussions was then organized, prioritized by the security needs of the projects (proximity to production readiness review and go-live date), and presented to Modernization Partner management to determine the best way to use resources to implement the resultant corrective actions. In doing these project drill-downs, we moved forward in determining what the enterprise should require for security before a system is authorized to operate, and we helped start the project manager security education process. We were also able to apply some security quick-fixes for projects going live in a matter of a few weeks.

Task Details

- Consolidated information from security status survey described in deliverable 59.1.3a
- Scheduled interviews with project managers for each project, in order to determine what specifically the project was about, when it went live, what type of data sensitivity and criticality issues existed, what security documentation had already been created, who the relevant security and system POCs were, etc. (see blank interview form)
- Collated interview data and prioritized projects by go-live dates and incomplete security actions
- Discussed and developed minimum-level SFA security requirements for PRR
- Provided recommendations to Modernization Partner management on what each project needed for security in order to be compliant with SFA PRR system security requirements
- Provided support for projects with imminent go-live dates, including IATO letter templates, security plan reviews, and risk assessment proposals (eCampus Based, SFA to the Internet and HR Modernization)
- Met with FMS project team to review security architecture recommendations
- Created a drawing of a potential Network Security Architecture following a DOD Defense in Depth model.
- Presented the Network Security Architecture to the Senior Technical Lead for Modernization in order to recommend that the Modernization Partner develop such a multi-point discipline for use across its projects

Task Status

Modernization Partner management was briefed on the security status of their upcoming projects, and what security documentation and risk assessments will meet the evolving SFA standards. Modernization Partner is currently in the process of implementing our recommendations across all projects. One project, SFA to the Internet, received a security plan review before their PRR and is in the process of setting up an independent risk assessment. Two others (HR Modernization and eCampus Based) are in the middle of setting up contracts for their risk assessments.

The Modernization Partner needs to plan for and implement two security architecture pieces of work: identification and authentication strategies across all modernization projects and standard service level agreements for network security (such as incident response and intrusion detection). This initial security integration effort has identified needs that should be championed in future tasks by a partnership of the OCIO and Modernization Partner.